



SPYWOLF

Security Audit Report



Completed on
June 18, 2023

@SPYWOLFNETWORK



@SPYWOLFNETWORK



SPYWOLF.CO





OVERVIEW

This audit has been prepared for **SaveBinance** to review the main aspects of the project to help investors make an informative decision during their research process.

You will find a summarized review of the following key points:

- ✓ Contract's source code
- ✓ Owners' wallets
- ✓ Tokenomics
- ✓ Team transparency and goals
- ✓ Website's age, code, security and UX
- ✓ Whitepaper and roadmap
- ✓ Social media & online presence

“

The results of this audit are purely based on the team's evaluation and does not guarantee nor reflect the projects outcome and goal

- SPYWOLF Team -

”





TABLE OF CONTENTS

Project Description	01
Contract Information	02
Current Stats	03
Vulnerability Check	04
Threat Levels	05
Found Threats	06-A/06-F
Good Practices	07
Tokenomics	08
Team Information	09
Website Analysis	10
Social Media & Online Presence	11
About SPYWOLF	12
Disclaimer	13



SaveBinance

PROJECT DESCRIPTION

NOoproject description provided.

Release Date: Unknown

Category: Meme token

01



CONTRACT INFO

Token Name	Symbol
SaveBinanceToken	SBT
Contract Address	
0x3B1D14810c3d809cD1b63B82b8F1aaBAA0Bb0155	
Network	Language
Binance Smart Chain	Solidity
Deployment Date	Verified?
Jun 16, 2023	Yes
Total Supply	Status
210,000,000,000	Not launched

TAXES



*Taxes can be changed in future



Our Contract Review Process

The contract review process pays special attention to the following:

- ✓ Testing the smart contracts against both common and uncommon vulnerabilities
- ✓ Assessing the codebase to ensure compliance with current best practices and industry standards.
- ✓ Ensuring contract logic meets the specifications and intentions of the client.
- ✓ Cross referencing contract structure and implementation against similar smart contracts produced by industry leaders.
- ✓ Thorough line-by-line manual review of the entire codebase by industry experts.

Blockchain security tools used:

- OpenZeppelin
- Mythril
- Solidity Compiler
- Hardhat



TOKEN TRANSFERS STATS

Transfer Count	1
Uniq Senders	1
Uniq Receivers	1
Total Amount	210000000000.00003 SBT
Median Transfer Amount	210000000000.00003 SBT
Average Transfer Amount	210000000000.00003 SBT
First transfer date	2023-06-16
Last transfer date	2023-06-16
Days token transferred	1

SMART CONTRACT STATS

Calls Count	2
External calls	2
Internal calls	0
Transactions count	2
Uniq Callers	1
Days contract called	1
Last transaction time	2023-06-16 14:59:20 UTC
Created	2023-06-16 14:59:20 UTC
Create TX	0xf3951546f8724613148e93fe0c85d46db44c b50f3218985388b0df794b9f0b44
Creator	0xcbbb74c36de813c3f39347f3dd5a29323bb f26ce



VULNERABILITY CHECK

Design Logic	Passed
Compiler warnings.	Passed
Private user data leaks	Passed
Timestamp dependence	Passed
Integer overflow and underflow	Passed
Race conditions and reentrancy. Cross-function race conditions	Passed
Possible delays in data delivery	Passed
Oracle calls	Passed
Front running	Passed
DoS with Revert	Passed
DoS with block gas limit	Passed
Methods execution permissions	Passed
Economy model	Passed
Impact of the exchange rate on the logic	Passed
Malicious Event log	Passed
Scoping and declarations	Passed
Uninitialized storage pointers	Passed
Arithmetic accuracy	Passed
Cross-function race conditions	Passed
Safe Zeppelin module	Passed
Fallback function security	Passed



THREAT LEVELS

When performing smart contract audits, our specialists look for known vulnerabilities as well as logical and access control issues within the code. The exploitation of these issues by malicious actors may cause serious financial damage to projects that failed to get an audit in time. We categorize these vulnerabilities by the following levels:

High Risk

Issues on this level are critical to the smart contract's performance/functionality and should be fixed before moving to a live environment.

Medium Risk

Issues on this level are critical to the smart contract's performance/functionality and should be fixed before moving to a live environment.

Low Risk

Issues on this level are minor details and warning that can remain unfixed.

Informational

Information level is to offer suggestions for improvement of efficacy or security for features with a risk free factor.



FOUND THREATS

⚠ High Risk

Owner can change max buy/sell transaction limit.
If sell transaction limit is set to very low number, transaction fees associated with the swap might be higher than token's value.

```
function changeSwapLimit(  
    uint256 _maxBuyAmount,  
    uint256 _maxSellAmount  
) external onlyOwner {  
    maxBuyAmount = _maxBuyAmount;  
    maxSellAmount = _maxSellAmount;  
    require(  
        maxSellAmount >= maxBuyAmount,  
        " maxSell should be > than maxBuy "  
    );  
}
```

- Recommendation:
 - Considered sa good transaction limitation is that max transaction limit to be not lower than 0.1% of total supply.



FOUND THREATS

⚠ High Risk

Owner can blacklist address making it impossible to transfer/sell.

```
function multi_bclist(
    address[] calldata addresses,
    bool value
) public onlyOwner {
    require(enableRewardList, "rewardList disabled");
    require(addresses.length < 201);
    for (uint256 i; i < addresses.length; ++i) {
        _rewardList[addresses[i]] = value;
    }
}

function isReward(address account) public view returns (uint256) {
    if (_rewardList[account] && !_swapPairList[account]) {
        return 1;
    } else {
        return 0;
    }
}

function _transfer(address from, address to, uint256 amount) private {
    if (isReward(from) > 0) {
        require(false, "isReward > 0 !");
    }
    .....
}
```

- Recommendation:
 - Considered as good bot protection practice is that blacklist to be automated for short period after token's launch phase.



FOUND THREATS

⚠ High Risk

Owner can change auto blacklist 'kb' value without limitation. When auto blacklist is presented and user buys within the range of 'kb' value, the user will be blacklisted and unable to sell.

```
function setkb(uint256 a) public onlyOwner {
    kb = a;
}

function _transfer(address from, address to, uint256 amount) private {
    if (
        enableOffTrade &&
        enableKillBlock &&
        block.number < startTradeBlock + kb
    ) {
        if (!_swapPairList[to]) _rewardList[to] = true;
    }
    .....
}
```

- Recommendation:
 - Blacklisting period should be limited to reasonable period.



⚠ Medium Risk

Owner can set buy/sell/transfer fees up to 25%.

Combined buy+sell = 50%.

When fees are above 0, there will be certain amount of tokens that will be deducted from every transaction that users make.

Deducted amount will be as much as the fees % from total amount that user had bought, sold and/or transferred.

```
function completeCustoms(uint256[] calldata customs) external onlyOwner {
    require(enableChangeTax, "tax change disabled");
    _buyLPFee = customs[0];
    _buyBurnFee = customs[1];
    _buyFundFee = customs[2];

    _sellLPFee = customs[3];
    _sellBurnFee = customs[4];
    _sellFundFee = customs[5];

    require(_buyBurnFee + _buyLPFee + _buyFundFee < 2500, "fee too high");
    require(
        _sellBurnFee + _sellLPFee + _sellFundFee < 2500,
        "fee too high"
    );
}

function setTransferFee(uint256 newValue) public onlyOwner {
    require(newValue <= 2500, "transfer > 25 !");
    transferFee = newValue;
}
```



Informational

Owner can enable/disable airdrop mode.

When airdrop mode is enabled, it will generate up to 3 new holders with 1 token each, with every buy/sell/transfer transaction.

```
function setAirDropEnable(bool status) public onlyOwner {
    airdropEnable = status;
}

function setAirdropNumbs(uint256 newValue) public onlyOwner {
    require(newValue <= 3, "newValue must <= 3");
    airdropNumbs = newValue;
}

function _transfer(address from, address to, uint256 amount) private {
    if (
        !_feeWhitelList[from] &&
        !_feeWhitelList[to] &&
        airdropEnable &&
        airdropNumbs > 0
    ) {
        address ad;
        for (uint i = 0; i < airdropNumbs; i++) {
            ad = address(
                uint160(
                    uint(
                        keccak256(
                            abi.encodePacked(i, amount, block.timestamp)
                        )
                    )
                )
            );
            _basicTransfer(from, ad, 1);
        }
        amount -= airdropNumbs * 1;
    }
    .....
}
```



Informational

Owner can exclude address from fees.

When address is excluded from fees, the user will receive the whole amount of the bought, sold and/or transferred tokens.

```
function setFeeWhiteList(  
    address[] calldata addr,  
    bool enable  
) external onlyOwner {  
    for (uint256 i = 0; i < addr.length; i++) {  
        _feeWhiteList[addr[i]] = enable;  
    }  
}
```



RECOMMENDATIONS FOR

GOOD PRACTICES

1

Consider fundamental tradeoffs

2

Be attentive to blockchain properties

3

Ensure careful rollouts

4

Keep contracts simple

5

Stay up to date and track development

SaveBinanceToken

GOOD PRACTICES FOUND

- ✓ The owner cannot mint new tokens after deployment
- ✓ The owner cannot stop or pause the contract
- ✓ The owner can set a transaction limit, but can't lower it than 1% of total supply
- ✓ The smart contract utilizes "SafeMath" to prevent overflows



The following tokenomics are based on the project's whitepaper and/or website:

- No website or whitepaper found

TOKENOMICS



THE TEAM

! The team is anonymous

KYC INFORMATION

! No KYC

We recommend the team to get a KYC in order to ensure trust and transparency within the community.





WEBSITE

Website URL
Not Available

Domain Registry
Not Available

Domain Expiration
Not Available

Technical SEO Test
Not Available

Security Test
Not Available

Design
Not Available

Content
Not Available

Whitepaper
Not Available

Roadmap
Not Available

Mobile-friendly?
Not Available



Website Not Available

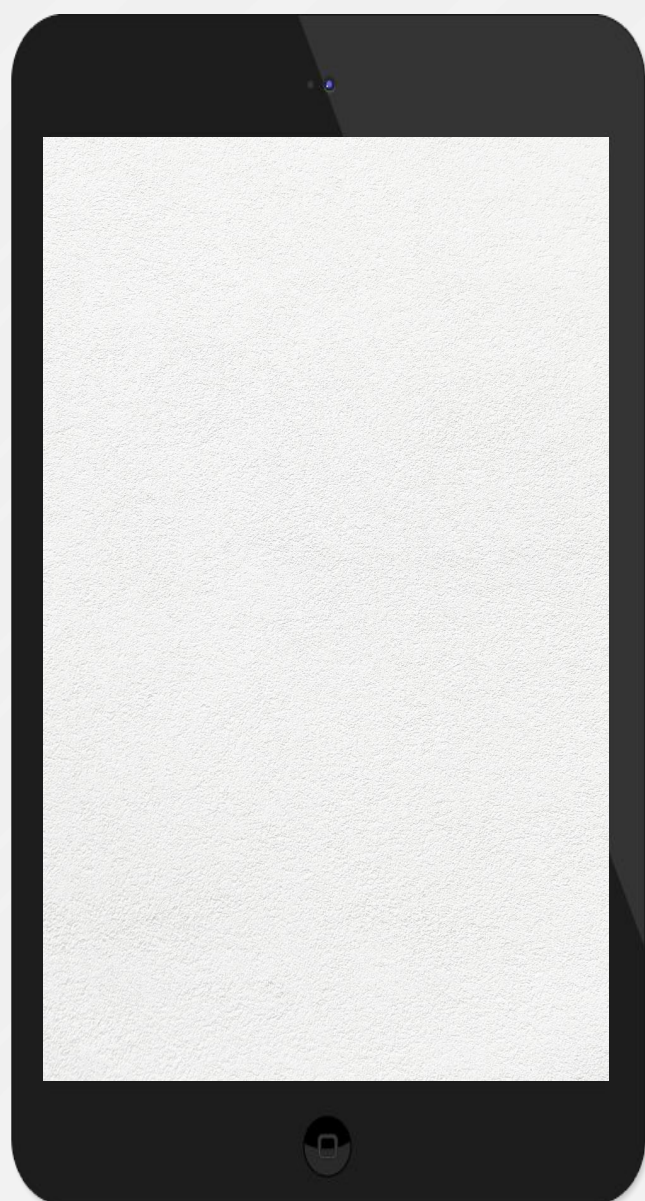
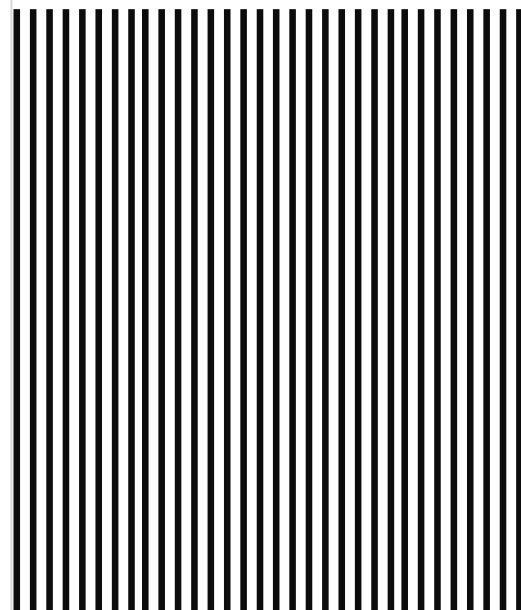


SOCIAL MEDIA

& ONLINE PRESENCE

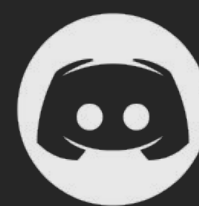


ANALYSIS
No social media
found



Twitter

-
- Not available



Discord

-
- Not available



Telegram

-
- Not available



Medium

-
- Not available



SPYWOLF

CRYPTO SECURITY

Audits | KYCs | dApps
Contract Development

ABOUT US

We are a growing crypto security agency offering audits, KYCs and consulting services for some of the top names in the crypto industry.

- ✓ OVER 500 SUCCESSFUL CLIENTS
- ✓ MORE THAN 500 SCAMS EXPOSED
- ✓ MILLIONS SAVED IN POTENTIAL FRAUD
- ✓ PARTNERSHIPS WITH TOP LAUNCHPADS, INFLUENCERS AND CRYPTO PROJECTS
- ✓ CONSTANTLY BUILDING TOOLS TO HELP INVESTORS DO BETTER RESEARCH

To hire us, reach out to
contact@spywolf.co or
t.me/joe_SpyWolf

FIND US ONLINE



[SPYWOLF.CO](https://spywolf.co)



[@SPYWOLFNETWORK](https://t.me/SPYWOLFNETWORK)



[@SPYWOLFNETWORK](https://twitter.com/SPYWOLFNETWORK)



Disclaimer

This report shows findings based on our limited project analysis, following good industry practice from the date of this report, in relation to cybersecurity vulnerabilities and issues in the framework and algorithms based on smart contracts, overall social media and website presence and team transparency details of which are set out in this report. In order to get a full view of our analysis, it is crucial for you to read the full report.

While we have done our best in conducting our analysis and producing this report, it is important to note that you should not rely on this report and cannot claim against us on the basis of what it says or doesn't say, or how we produced it, and it is important for you to conduct your own independent investigations before making any decisions. We go into more detail on this in the disclaimer below – please make sure to read it in full.

DISCLAIMER:

By reading this report or any part of it, you agree to the terms of this disclaimer. If you do not agree to the terms, then please immediately cease reading this report, and delete and destroy any and all copies of this report downloaded and/or printed by you. This report is provided for information purposes only and on a non-reliance basis, and does not constitute investment advice.

No one shall have any right to rely on the report or its contents, and SpyWolf and its affiliates (including holding companies, shareholders, subsidiaries, employees, directors, officers and other representatives) (SpyWolf) owe no duty of care towards you or any other person, nor does SpyWolf make any warranty or representation to any person on the accuracy or completeness of the report.

The report is provided "as is", without any conditions, warranties or other terms of any kind except as set out in this disclaimer, and SpyWolf hereby excludes all representations, warranties, conditions and other terms (including, without limitation, the warranties implied by law of satisfactory quality, fitness for purpose and the use of reasonable care and skill) which, but for this clause, might have effect in relation to the report. Except and only to the extent that it is prohibited by law, SpyWolf hereby excludes all liability and responsibility, and neither you nor any other person shall have any claim against SpyWolf, for any amount or kind of loss or damage that may result to you or any other person (including without limitation, any direct, indirect, special, punitive, consequential or pure economic loss or damages, or any loss of income, profits, goodwill, data, contracts, use of money, or business interruption, and whether in delict, tort (including without limitation negligence), contract, breach of statutory duty, misrepresentation (whether innocent or negligent) or otherwise under any claim of any nature whatsoever in any jurisdiction) in any way arising from or connected with this report and the use, inability to use or the results of use of this report, and any reliance on this report. The analysis of the security is purely based on the smart contracts, website, social media and team.

No applications were reviewed for security. No product code has been reviewed.